UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte DEEPAK GUPTA and VAMSAVARDHANA R. CHILLAKURU

Appeal 2007-1507
Application 09/626,637
Technology Center 2100

Decided: September 25, 2007

Before MAHSHID D. SAADAT, ALLEN R. MacDONALD,
and ROBERT E. NAPPI, *Administrative Patent Judges.*

SAADAT, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's Non-Final Rejection of claims 1-6 and 11-19, which constitute all of the claims pending in this application, as claims 7-10 have been canceled. We have jurisdiction under 35 U.S.C. § 6(b).

We reverse.

Appellants invented a method and a system to solve the problem of expired digital certificates issued by a certifying authority in a secure communication environment over a public network (Specification 1). According to Appellants, the certifying authority provides a server certifying authority chain certificate (SCAC certificate) using its new keys to validate the previously issued server certificate (Specification 3).

Independent Claim 1 is representative of the claims on appeal and reads as follows:

> 1. A method for enabling use by a browser of valid authentication certificates in relation to a transaction between the browser and a server when a private key and public key of a certifying authority of the server has expired, comprising:
>
> receiving an original authentication certificate together with a server certifying authority chain (SCAC) certificate by the browser from the server during a[] SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by the server from the certifying authority;
>
> verifying by the browser the original authentication certificate using the expired public key of the certifying authority; and
>
> verifying by the browser the SCAC certificate using a new public key of the certifying authority.

The Examiner relies on the following prior art in rejecting the claims:

Weinstein	US 6,094,485	Jul. 25, 2000
Perlman	US 6,230,266 B1	May 8, 2001
Lewis	US 6,233,565 B1	May 15, 2001
Kramer	US 6,324,525 B1	Nov. 27, 2001

Claims 1, 5[1], 6, 11-13, and 17-19 stand rejected as being unpatentable under 35 U.S.C. § 103(a) over Lewis and Weinstein.

Claims 2, 3, 14, and 15 stand rejected as being unpatentable under 35 U.S.C. § 103(a) over Lewis, Weinstein, and Perlman.

Claim 4 stands rejected as being unpatentable under 35 U.S.C. § 103(a) over Lewis, Weinstein, and Kramer.

Claim 16 stands rejected as being unpatentable under 35 U.S.C. § 103(a) over Lewis, Weinstein, Perlman, and Kramer.

We reverse.

ISSUE

Appellants argue that the combination of Lewis and Weinstein cannot be properly combined to teach or suggest receiving the old certificate and the new certificate by the browser from the server because receiving the original authentication certificate together with the SCAC certificate is not relevant to the teachings of Lewis (Br. 6-8). Therefore, the issue on appeal turns on whether a preponderance of the evidence before us shows that under 35 U.S.C. § 103, the combination of Lewis and Weinstein teaches or suggests the claimed subject matter and specifically receiving the old and the new certificate together by the browser from the server.

---

[1] Claim 4 was mistakenly included in the statement of rejection (Non-Final Rejection, mailed Aug. 11, 2005).

FINDINGS OF FACT

The following findings of fact (FF) are relevant to the issue involved in the appeal and are believed to be supported by a preponderance of the evidence.

1. Lewis describes the authentication protocol entered by the server when a client establishes connection (col. 28, ll. 50-52), wherein a key generation routine produces the server's public/private authentication key having an expiration period, which will get replaced with new authentication keys (col. 30, ll. 13-21).

2. Lewis discloses that when a certificate expires, the USPS certification authority will issue a new certificate and sign it with the old certificates matching private key. The USPS Certification Authority (CA) will send a new certificate signed with the CA's new private key to the *server* 4. The server 4 will validate the certificate for authenticity by first checking to ensure that the new CA certificates public key authenticates the included signature (col. 30, ll. 36-50).

3. Weinstein provides a process, referred to as the Secure Sockets Layer (SSL) step up, which allows an exportable SSL client to negotiate an encrypted session using strong encryption with a server if the server is approved for the step up (col. 1, ll. 35-39).

4. The process of the SSL step up in Weinstein involves performing an SSL handshake twice. The process begins when a user desires to establish a session with a server. If the server is approved, the client initiates a second handshake, this time allowing stronger cipher suites. The

result of the second handshake is an SSL session that uses strong encryption (Figure 3; col. 1, ll. 50-59).

5. Weinstein performs multiple handshakes during long lived Secure Sockets Layer (SSL) sessions to allow for re-keying for long lived sessions which, in turn, ensures the strength of the SSL session if it is followed by a second handshake (col. 3, ll. 44-52).

6. As depicted in Figure 2 of Weinstein, server's certificate is checked using the server's certificate chain such as the server's certificate, CA certificates, and a trusted root CA certificate (col. 3, ll. 54-60). The server's certificate and any intermediate CA certificates must contain the certificate extension before the server is approved for SSL (col. 3, l. 63 through col. 4, l. 7).

PRINCIPLES OF LAW

The examiner bears the burden of establishing a prima facie case of obviousness. *In re Rijckaert*, 9 F.3d 1531, 1532, 28 USPQ2d 1955, 1956 (Fed.Cir. 1993); *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed.Cir. 1992). Only if this burden is met does the burden of coming forward with rebuttal argument or evidence shift to the applicant. *Rijckaert*, 9 F.3d at 1532, 28 USPQ2d at 1956. When the references cited by the examiner fail to establish a prima facie case of obviousness, the rejection is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). *See alsoIn re Zurko*, 258 F.3d 1379, 1383, 1385, 59 USPQ2d 1693, 1695, 1697 (Fed. Cir. 2001) (reversing as unsupported by substantial evidence a finding of motivation to combine cited references, where the Board adopted Examiner's unsupported assertion

that claim limitation missing from cited references was "basic knowledge" and it "would have been nothing more than good common sense" to combine the references, and explaining that "[t]his assessment of basic knowledge and common sense was not based on any evidence in the record").

Further, a rejection based on section 103 must rest upon a factual basis rather than conjecture, or speculation. "Where the legal conclusion [of obviousness] is not supported by facts it cannot stand." *In re Warner*, 379 F.2d 1011, 1017, 154 USPQ 173, 178 (CCPA 1967). *See also In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006).

ANALYSIS

Appellants specifically argue that when a certificate expires in Lewis, the certification authority will issue a new certificate, sign it with the old certificate's matching private key, and send it to server 4, where the certificate is validated (Br. 6-8). Appellants further argue that the certificates are not only received by the server instead of the browser, but also cannot be reasonably received together since the new one replaces the old one only after the old certificate expires (Br. 8). The Examiner argues that the combination of Lewis and Weinstein provides for receiving multiple certificates within one transmission (Answer 18) while the server and client roles are interchangeable based on which system requests services (Answer 19).

We agree with Appellants and find that by issuing a new certificate when the old one expires, Lewis actually replaces the old certificate with a

new one signed with the certifying authority's new private key (FFs 1 & 2). At this point, as argued by Appellants (Br. 8), the server already has the old certificate and there is no need for it to receive an old expired certificate. We also agree with Appellants that the server and the browser of Lewis are not interchangeable since Lewis intends for the server to perform the related server functions for a group of clients. Furthermore there is no indication in Lewis that the received certificates were transmitted to any browser (FF 2).

We further agree with Appellants' assertion (Reply Br. 6) that Weinstein provides multiple certificates to verify a server by a client (FF 4), whereas the old and the new certificates in Lewis are to verify a Certification Authority by a server. Furthermore, the multiple handshaking during a Secure Sockets Layer (SSL) session in Weinstein is not due to expiration of the certificate, but to ensure that the strength of the SSL session is not weakened (FFs 5 & 6).

Therefore, we find that the Examiner's rejection rests on speculation and less than substantial evidence and thus, fails to provide sufficient support for finding claim 1 and claim 6 and 13, which include similar limitations, as well as claims 5, 11, 12, and 17-19, dependent thereon unpatentable for obviousness under 35 U.S.C. § 103(a) over Lewis and Weinstein.

With respect to the rejection of the remaining claims over the various combinations of Lewis and Weinstein with Kramer and Perlman, we note that the Examiner has not pointed to any additional teachings in these references that would have overcome the deficiencies of Lewis and Weinstein discussed above with respect to the base claims. As such, we

cannot sustain the 35 U.S.C. § 103 rejection of claims 2, 3, 14, and 15 over Lewis, Weinstein, and Perlman, of claim 4 over Lewis, Weinstein, and Kramer, and of claim 16 over Lewis, Weinstein, Perlman, and Kramer.

DECISION

The decision of the Examiner rejecting claims 1-6 and 11-19 under 35 U.S.C. § 103 is reversed.

REVERSED

tdl/gvw

SCHMEISER, OLSEN & WATTS
22 CENTURY HILL DRIVE
LATHAM NY 12110